

1 ELECTRONIC CONTENTS PROVING METHOD AND SYSTEM, AND  
2 STORAGE MEDIUM FOR STORING PROGRAM THEREFOR

3 [Field of the Invention]

4 The present invention relates to a method and a system  
5 for proving electronic content and a storage medium for  
6 storing a program therefor, and particularly to a  
7 technique that can effectively prove openness of subject  
8 electronic content for perusal and subject electronic  
9 content has not been altered.

10 [Background Art]

11 It is generally considered common knowledge that  
12 information concerning ideologies, technical ideas, such  
13 as inventions, and other documents and drawings are  
14 publicly disclosed by being issued as printed matter  
15 and/or by being included in publications wherein  
16 characters and graphic illustrations are printed on paper  
17 media. Such printed matter is usually accepted as  
18 written proof, and is also, once authenticity has been  
19 established, admissible as documentary evidence, as  
20 evidence for a contract freely entered into by two or  
21 more parties, or as evidence for administrative  
22 procedures such as probative matter detailing lack of  
23 novelty of invention, as set forth in Japanese Patent Law  
24 section 29, subsection 1, paragraph 3 and section 30.,  
25 etc. The availability of printed matter or of verifiable

1 evidence that information has been published can be  
2 easily attested by providing the printed matter itself  
3 and publication dates. And proof that there has been no  
4 alteration of meaning can be demonstrated by providing  
5 examples showing that the content of printed matter has  
6 not been changed.

7 In accordance with recent developments in techniques  
8 employed on the Internet, opportunities have increased  
9 whereby information (content) that conventionally is  
10 disclosed using printed matter is laid open for perusal  
11 by the public using the Internet. Since such electronic  
12 content is thus disclosed as it would be included in  
13 printed matter, interested parties desire to utilize as  
14 evidence, as is described above, content opened for  
15 perusal in this fashion.

16 An electronic notary system, such as "www.surety.com", is  
17 well known that can be used to affirm the presence of  
18 electronic contents. The electronic notary system  
19 converts the electronic contents into hash code, and  
20 announces the hash code in a newspaper to notify  
21 unspecified third parties of the existence of the  
22 electronic content, and establishes the fact that the  
23 electronic content thereby made available. Thus, facts  
24 written as electronic content can be proved, and when,  
25 for example, a copyright is included in the electronic  
26 contents, the inclusion of the copyright can be attested.

27 However, when electronic content is to be used as  
28 evidence, as is described above, this, unlike the use of  
29 printed matter for a like purpose, produces a unique

1 problem, i.e., questions as to the probative force of  
2 electronic content have arisen. Since a publisher (a  
3 homepage creator) independently uploads electronic  
4 content to a homepage, it would be difficult to prove the  
5 publication of such content and to furnish a publication  
6 date without obtaining certification provided by a third  
7 party, such as a notary public. Further, since the  
8 operation of a homepage is generally a voluntary  
9 activity, a homepage operator can freely alter content,  
10 so that the probative force as to non-alteration of the  
11 content is weakened without the provision of third party  
12 authentication. While means for proving the existence of  
13 electronic content is available, as is described above,  
14 probative force equivalent to that attributable to  
15 printed matter can not be acquired merely by establishing  
16 the fact that electronic content is available. For  
17 example, in order to confirm that a technical idea for  
18 electronic content (an invention) is, as stated in  
19 Japanese Patent Law section 29, subsection 1, paragraph  
20 3, "inventions which have been described in a publication  
21 distributed in Japan or elsewhere or inventions which  
22 became available to the general public through  
23 telecommunication lines in such places prior to the  
24 filing of the patent application", according to the  
25 "Operational Guidelines on Treatment of Technical  
26 information disclosed on the Internet as Prior Art"  
27 provided by the Japanese Patent Office, the following is  
28 required: "information should be available to the  
29 public", i.e., information should be so distributed and  
30 stored that it can be obtained and perused by any and all  
31 unspecified persons, and that electronic technical  
32 information cited when filing for a patent application

1 should be written exactly as previously described.  
2 However, the conventional technique can not be used to  
3 prove openness for perusal (availability to the public)  
4 nor that at the time of the filing of the patent  
5 application no content alteration has been made.

6 Openness for perusal (availability to the public) and  
7 that no electronic content has been altered are to be  
8 proved not only for claiming as prior art for the Patent  
9 Law. However, using the conventional technique, only the  
10 fact that specific electronic content was available on a  
11 specific date can be proved; it is difficult to prove  
12 openness for perusal and that the content was not altered  
13 (completeness and legality).

14 [Summary of the Invention]

15 It is one object of the present invention to provide  
16 means for attesting to the openness for perusal of  
17 electronic contents that are present on a network.

18 It is another object of the present invention to provide  
19 means for attesting there has been no alteration of the  
20 electronic content that is present on a network.

21 It is an additional object of the present invention to  
22 provide the probative force necessary to demonstrate the  
23 openness for perusal and lack of alteration of the  
24 electronic content.

25 An overview of the present invention will now be  
26 presented. Specifically, according to the invention, for

1 a user who desires to prove the openness for perusal of  
2 electronic contents, a plurality of witnesses or  
3 certificate generators are selected from proposed  
4 witnesses registered in advance, and a certificate of  
5 having obtained the electronic content is issued by the  
6 selected witnesses or certificate generators, so that the  
7 openness for perusal of the electronic contents can be  
8 proved. The witnesses or the certificate generators can  
9 be selected at random from a group of registered  
10 witnesses (including certificate generators). In this  
11 case, it is preferable that a large group be registered  
12 and be prepared to guarantee randomness. In this  
13 invention, a proxy server possessing a certificate  
14 generation function can be employed as a certificate  
15 generator.

16 According to the present invention, witnesses or  
17 certificate generators (third parties) that are unrelated  
18 not only to a user but also to a service provider issue  
19 certificates. Thus, since the certificates are issued by  
20 witnesses that is not related to a user they acquire a  
21 higher probative force. In addition, according to the  
22 present invention, many certificates can be collected via  
23 a computer network, such as the Internet, and the  
24 probative force increases as the number of witnesses  
25 (certificates) grows.

26 Brief Description of the Drawings:

27 Fig. 1 is a conceptual diagram for explaining an example  
28 proving system according to a first embodiment of the

1 present invention.

2 Fig. 2 is a block diagram showing an example service  
3 provider and an example certificate generator for the  
4 system according to the first embodiment.

5 Fig. 3 is a block diagram showing an example certificate  
6 request receiver and an example certification manager.

7 Fig. 4 is a block diagram showing an example certificate  
8 generation manager, an example certification generation  
9 processor and an example electronic signature generator.

10 Fig. 5 is a block diagram showing another example  
11 certificate generation manager, another example  
12 certification generation processor and another electronic  
13 signature generator.

14 Fig. 6 is a flowchart showing the general processing  
15 performed for the method of this invention.

16 Fig. 7 is a diagram showing a screen for an example usage  
17 request dialogue when a user issues a service request.

18 Fig. 8 is a detailed flowchart showing a user  
19 verification step.

20 Fig. 9 is a detailed flowchart showing a user's request  
21 analyzation step.

22 Fig. 10 is a detailed flowchart showing a registered  
23 member selection step.

24 Fig. 11 is a detailed flowchart showing a certification  
25 process.

26 Fig. 12 is a diagram showing a screen for an example  
27 intent confirmation dialogue used for a witness process.

28 Fig. 13A is a block diagram showing a system for use of  
29 an external clock for time synchronization.

30 Fig. 13B is a flowchart showing a time synchronization  
31 method.

32 Fig. 14A is a block diagram showing a system for use of

1 an internal clock for time synchronization.  
2 Fig. 14B is a flowchart showing a time synchronization  
3 method.  
4 Fig. 15 is a detailed flowchart showing a certificate  
5 generation step.  
6 Fig. 16 is a diagram showing a screen for a certificate  
7 generation dialogue before an electronic signature is  
8 provided.  
9 Fig. 17 is a detailed flowchart showing an electronic  
10 signature step.  
11 Fig. 18 is a detailed flowchart showing a certificate  
12 acceptance step.  
13 Fig. 19 is a diagram showing a screen for the final  
14 production of an example certificate by a service  
15 provider.  
16 Fig. 20 is a diagram showing a screen for the final  
17 production of another example certificate by a service  
18 provider.  
19 Fig. 21 is a detailed flowchart showing a certificate  
20 dispatching step.  
21 Fig. 22A is a block diagram showing a witness  
22 registration system.  
23 Fig. 22B is a flowchart showing a witness registration  
24 method.  
25 Fig. 23 is a conceptual diagram for explaining an example  
26 proving system according to a second embodiment of the  
27 present invention.  
28 Fig. 24 is a block diagram showing an example service  
29 provider and an example certificate generator for the  
30 system according to the second embodiment.  
31 Fig. 25 is a block diagram showing an example certificate  
32 generation manager and an example certification

1 generation processor.  
2 Fig. 26 is a conceptual diagram for explaining an  
3 additional example proving system according to the  
4 present invention.  
5 Fig. 27 is a conceptual diagram for explaining a further  
6 example proving system according to the present  
7 invention.

8 [Description of the Symbols]

9 10: Service provider  
10 11: User  
11 12: Registered member group  
12 12a: Witness  
13 12a: Certificate generator  
14 13: Content transmitter  
15 14: Electronic content  
16 21: Certificate request receiver  
17 22: Certificate transmitter  
18 23: Certification manager  
19 23a: Time synchronization unit  
20 24: Communication unit  
21 25: Registered member selector  
22 26: Registered member database  
23 27: Clock  
24 28: Electronic content acquisition unit  
25 29: Communication unit  
26 30: Certificate generation manager  
27 31: Electronic content acquisition unit  
28 32: Clock (internal clock)  
29 33: Certification generation processor  
30 34: Electronic signature generator  
31 36: Public key authentication server



1 40: Registered member database  
2 41: Witness registration manager  
3 42: Communication unit  
4 43: Communication unit  
5 44: Witness registration unit  
6 81: Button  
7 211: User address  
8 212: Content address  
9 213: Witness condition  
10 214: Certificate period  
11 215: Certificate of accuracy  
12 231: User verification unit  
13 232: User request analyzation unit  
14 233: Usage history file  
15 234: Certificate dispatching unit  
16 235: Certificate acceptance unit  
17 236: Witness process requesting unit  
18 237: Time manager  
19 302: Electronic content  
20 303: Time  
21 331: Data set  
22 332: Certificate  
23 341: Hash function unit  
24 342: Hash code  
25 343: Secret key encryption means  
26 344: Encrypted hash code  
27 345: Public key  
28 346: Encrypted content address  
29 347: Encrypted electronic content  
30 348: Encryption time  
31 800: Dialogue  
32 800: Input dialogue

1 801: Input field  
2 802 to 809: Input field  
3 810: OK button  
4 811: Cancel button  
5 820: Dialogue  
6 821: OK button  
7 822: Cancel button  
8 830: Dialogue box  
9 831: Field  
10 832: Field  
11 834: OK button  
12 835: Cancel button  
13 840: Frame  
14 841: File  
15 842: Field  
16 843: Field  
17 850: Frame  
18 851: Field  
19 852 to 855: Field  
20 856: Field  
21 900: Notary service provider (electronic notary service)  
22 901: Witness profile  
23 902: Data  
24 903: Certificate

25 [Preferred Embodiments]

26 The preferred embodiments of the present invention will  
27 now be described in detail. It should be noted, however,  
28 that the present invention should not be construed as  
29 being limited to the embodiments included in the  
30 following explanation, but that additionally it can be

1 implemented by various other embodiments. It should also  
2 be noted that throughout the following explanation the  
3 same reference numerals are used for corresponding or  
4 identical components.

5 In the following embodiments, methods and systems will  
6 mainly be described. However, as will be apparent to one  
7 having ordinary skill in the art, the present invention  
8 can be carried out not only by a method and a system, but  
9 also by a storage medium on which computer executable  
10 program code is stored. Therefore, the present invention  
11 can be provided as hardware or as software, or as a  
12 combination of the two. The storage medium used for  
13 storing program code can be an arbitrary  
14 computer-readable storage medium, such as a hard disk, a  
15 CD-ROM, an optical storage device, or a magneto-optical  
16 disk.

17 For the invention, an applicable computer system  
18 comprises a central processing unit (CPU), a main memory  
19 (random access memory (RAM)) and nonvolatile memory (read  
20 only memory (ROM)), all of which are interconnected by a  
21 bus. A co-processor, an image accelerator, a cache  
22 memory and an input/output control unit (I/O) are also  
23 connected to the bus. And since it is natural that  
24 hardware resources with which a computer system is  
25 generally equipped should be included, an external  
26 storage device, a data input device, a display device and  
27 a communication controller may be connected to the bus  
28 via an appropriate interface. The external storage  
29 device can be a hard disk device, but is not thus  
30 limited, and can include a semiconductor storage device,

1 such as a magneto-optical storage device, an optical  
2 storage device or a flash memory. A read only storage  
3 device, such as a CD-ROM, can also serve as an external  
4 storage device, if it is employed only for reading data  
5 or a program. Further, the data input device can be, for  
6 example, a keyboard or a pointing device, such as a  
7 mouse, or can even be a voice input device. And a CRT, a  
8 liquid crystal display device or a plasma display device  
9 can be employed as a display device. Finally, the  
10 computer system in the embodiments can be a personal  
11 computer, a workstation, a mainframe computer or some  
12 other type of programmable machine.

13 In the embodiments, for communication between computer  
14 systems, mainly the Internet is employed, but a LAN or a  
15 WAN to which a plurality of computer systems are  
16 connected may be employed instead, and a communication  
17 line used for this connection may be either a special  
18 network line or a public network line. Further, although  
19 in the embodiments multiple computer systems are  
20 employed, the present invention may be implemented by a  
21 single computer.

22 The program used by one computer system may be recorded  
23 in another computer. That is, a remote computer can  
24 perform distributed processing for one part of the  
25 program used by the computer system. It should be noted  
26 that the DNS or the URL can be referred to the program  
27 that is stored in another computer system.

28 When mention is made of the accessing of the Internet, as  
29 it is in this specification, the remark applies both to

1 intranets and to extranets. The term "computer network"  
2 includes both a publicly accessible computer network and  
3 a privately accessible computer network.

4 (First Embodiment)

5 Fig. 1 is a conceptual diagram for explaining an example  
6 proof system according to one embodiment of the present  
7 invention. The system in this embodiment includes a  
8 service provider 10, a user 11, a registered member group  
9 12, which comprises a group of witnesses or certificate  
10 generators 12a, a content transmitter 13, and electronic  
11 content 14. The above described general computer system,  
12 which is connected to the Internet, is employed as the  
13 service provider 10, the user 11, a witness or a  
14 certificate generator 12a, and the content transmitter  
15 13. HTTP (Hypertext Transfer Protocol), for example, is  
16 employed for the transmission of data between the  
17 computer systems, and data written in HTML (Hypertext  
18 Markup Language) can be displayed using an appropriate  
19 browser.

20 The service provider 10 is means for proving that  
21 electronic content has been opened for perusal or that  
22 the electronic content has not been altered. The service  
23 provider 10 will be described in detail later.

24 The user 11, who accepts a service for the proving of the  
25 electronic content, employs the above described computer  
26 system to transmit a service request (client request) to  
27 the service provider 10. Upon receipt of the service  
28 request, the computer system of the service provider 10  
29 functions as a server and prepares a document using HTML

1 or XML (Extensible Markup Language) that it returns to  
2 the computer system of the user 11, whereat it is  
3 displayed the screen of the display device.

4 The witness or certificate generator 12a is a person or a  
5 computer system that issues a certificate for the  
6 electronic content upon the receipt of a proof request  
7 from the service provider 10. The witness issues a  
8 certificate by operating a computer system, the  
9 certificate generator 12a. The certificate generator 12a  
10 may not only be operated by the witness, but may itself  
11 also serve as a proxy server. When serving as a proxy  
12 server, the certificate generator 12a automatically  
13 issues a certificate, without requiring the intervention  
14 of a human. The certificate generator 12a will be  
15 described in detail later.

16 The content transmitter 13 is a computer system that  
17 stores electronic content 14 to be proved. The  
18 electronic content 14 can be, for example, a document  
19 file, such as a homepage that is displayed by a common  
20 browser. However, the electronic content 14 is not  
21 limited to a document file (e.g., an HTML document or an  
22 XML document) displayed by a browser, but may be a data  
23 file that can be transferred using FTP (File Transfer  
24 Protocol), data posted on a bulletin board used for PC  
25 communication service, or data in a message dispatched to  
26 a network news destination. The electronic content 14  
27 can be any electronically recorded data; even data  
28 printed on paper can be included in the electronic  
29 content 14 classification, just so long as the data can  
30 be converted into electronic data using an image reader.

Fig. 2 is a block diagram showing examples for the service provider 10 and the certificate generator 12a of the system according to the first embodiment. Fig. 3 is a block diagram showing an example certificate request receiver and an example certification manager. Fig. 4 is a block diagram showing an example certificate generation manager, an example certification generation processor and an example electronic signature generator. As is shown in Fig. 2, the service provider 10 comprises a certificate request receiver 21, a certificate transmitter 22, a certification manager 23, a communication unit 24, a registered member selector 25, a registered member database 26, a clock 27, and an electronic content acquisition unit 28. The certificate generator 12a includes a communication unit 29, a certificate generation manager 30, an electronic content acquisition unit 31, a clock 32, and a certification generation processor 33 and an electronic signature generator 34.

The individual sections or the more detailed portions of these sections are implemented as software functions that are provided as programs for the computer system. The software functions can be obtained by using the hardware resources of the computer system.

The certificate request receiver 21 receives from the user 11 a service request that, as is shown in Fig. 3, includes a user address 211, a content address 212, a witness condition 213, a certificate period 214 and a certificate of accuracy 215.

1 The certificate transmitter 22 transmits the certificate  
2 that is finally prepared to the user 11. When the user  
3 11 and the service provider 10 are interconnected via the  
4 Internet, the certificate may be transmitted as an HTML  
5 document using HTTP, or may be transmitted using FTP or  
6 as an e-mail.

7 The certification manager 23 manages the certification  
8 process performed by the service provider 10. As is  
9 shown in Fig. 3, the certification manager 23 includes a  
10 user verification unit 231, a user request analyzation  
11 unit 232, a usage history 233, a certificate dispatching  
12 unit 234, a certificate acceptance unit 235, a witness  
13 process requesting unit 236 and a time manager 237. The  
14 functions of the individual sections will be described in  
15 detail later during the explanation of the method of the  
16 invention.

17 The communication unit 24 has a control function for  
18 communicating with the certificate generator 12a, which  
19 is the computer system of a witness or which itself  
20 serves as a proxy server. A certificate request is  
21 transmitted via the communication unit 24 to the  
22 certificate generator 12a. And for communication  
23 performed via the Internet, the certificate request may  
24 be transmitted as an HTML document using HTTP, or may be  
25 transmitted using FTP or as an e-mail.

26 In accordance with the analyzation results obtained in  
27 response to the request by the user 11 and transmitted to  
28 the user request analyzation unit 232, the registered



1 member selector 25 selects a required number of  
2 appropriate registered members from the registered member  
3 database 26. During this process, a determination is  
4 made as to whether humans or proxy servers should be  
5 selected as registered members, or whether the number of  
6 registered members should be limited in accordance with  
7 an area requirement. When a registered member is a  
8 human, age, gender or occupation limitations may be  
9 applied during the process to determine whether the  
10 selection of the member is appropriate. Note, however,  
11 that the conditions listed here are merely examples, and  
12 that other conditions may be added. In the registered  
13 member database 26, not only is the type of registered  
14 member (a human or a proxy server) recorded, but also the  
15 district, the age, the gender, the occupation and other  
16 necessary information, such as a certification history,  
17 are entered. Further, the registered member database 26  
18 need not be stored in the service provider 10, but may be  
19 recorded in an external storage area identified by an  
20 address, such as a URL.

21 While the clock 27 is incorporated in the computer  
22 system, the clock 27 need not be internally provided for  
23 the service provide 10, and the clock of an external  
24 service provider may be referred to.

25 The electronic content acquisition unit 28 is used when  
26 the service provider 10 can not itself obtain at the  
27 content address 212 the electronic content that is  
28 included in the service request. The electronic content  
29 acquisition unit 28 includes a function for obtaining  
30 data based on the protocol that matches the recorded

1 electronic content. For example, if the electronic  
2 content is an HTML document, the electronic content  
3 acquisition unit 28 employs HTTP to acquire the  
4 electronic data. The electronic content obtained here is  
5 used to determine whether this content is identical to  
6 the electronic content obtained by a witness or a proxy  
7 server.

8 The communication unit 29 has a control function for  
9 communicating with the computer system of the service  
10 provider 10, and has the same configuration as the  
11 communication unit 24. The certificate generation manager  
12 30, in the certificate generator 12a of the witness or  
13 the proxy server, manages the preparation of a  
14 certificate. As is shown in Fig. 4, the certificate  
15 generation manager 30 refers to the content address 212  
16 included in the certificate request, and obtains  
17 electronic content 302 via the electronic content  
18 acquisition unit 31. The certificate generation manager  
19 30 also obtains a time 303 from the clock 32. The  
20 electronic content acquisition unit 31 has the same  
21 configuration as the electronic content acquisition unit  
22 28.

23 While the clock 32 is incorporated into the certificate  
24 generator 12a, it is not necessarily provided for the  
25 certificate generator 12a, and a clock belonging to an  
26 external service provider may be referred to.

27 The certification generation processor 33 prepares a  
28 certificate. The certification generation processor 33  
29 produces the content address 212 included in the

1 certificate request, the electronic content 302 that has  
2 been obtained and the time 303 that is obtained as a set  
3 of data 331, and transmits the data 331 to the electronic  
4 signature generator 34.

5 The electronic signature generator 34 includes a function  
6 for providing an electronic signature for the data set  
7 331. The electronic signature generator 34 employs a  
8 hash function unit 341 to generate hash code 342 using  
9 the data set 331. Thereafter, inherent secret key  
10 encryption means 343 encrypts the hash code 342, and an  
11 encrypted hash code 344 is transmitted to the  
12 certification generation processor 33, along with a  
13 public key 345 registered in a public key authentication  
14 server 36.

15 The certification generation processor 33 adds the  
16 encrypted hash code 344 and the public key 345 to the  
17 data set 331 (including the content address 212, the  
18 electronic content 302 and the time 303) to generate a  
19 certificate 332.

20 Since the data set 331, which includes the electronic  
21 content 302, that generally has a large volume is  
22 converted into the hash code 342 that has a small volume,  
23 whether or not the contents are identical can be easily  
24 determined. That is, when the data are converted into  
25 hash code, a small difference between the data before  
26 conversion appears as a large change in the hash code.  
27 Thus, when multiple certificates are compared, the  
28 alteration of the content appears as a large change in  
29 the hash code.

1 In this embodiment the hash code 342 is employed;  
2 however, another data conversion method may be employed  
3 whereby data can be uniquely represented. Further, as is  
4 shown in Fig. 5, the hash code may not be employed. In  
5 this case, to obtain the certificate 332, the set of data  
6 331 may be encrypted using the secret key encryption  
7 means 343, and a public key 345 may be added to an  
8 encrypted content address 346, encrypted electronic  
9 content 347 and an encryption time 348.

10 The proving method for this invention will now be  
11 described. The overview of the proving method of this  
12 invention that follows is presented while referring to  
13 Fig. 1. The user 11 requests a service from the service  
14 provider 10 (step (1) in Fig. 1). To issue the service  
15 request, the user 11 transmits the address of the content  
16 transmitter 13 that distributes the electronic content 14  
17 that is to be proved, and if necessary, also transmits  
18 various conditions to be applied for the selection of the  
19 witnesses.

20 From the registered member group 12, which consists of  
21 witnesses or certificate generators 12a that have been  
22 registered in advance, the service provider 10 selects at  
23 random witnesses or certificate generators 12a that match  
24 the conditions (step (2)). During this process, the  
25 service provider 10 employs the addresses to be proved of  
26 the selected witnesses or certificate generators 12a to  
27 request that they to prove that the content was opened  
28 for public perusal.

1 The witnesses or the proxy servers (the certificate  
2 generators 12a) request that the content transmitter 13  
3 (step (3)) transmit the content to them.

4 If the content has already been opened for perusal, the  
5 electronic content 14 to be proved is transmitted to the  
6 witnesses or the proxy servers (the certificate  
7 generators 12a) (step (4)).

8 When the witnesses or certificate generators 12a have  
9 scanned the electronic content 14, they add time stamps  
10 to the electronic content 14, perform a non-variable  
11 process, such as electronic signing, that the service  
12 provider 10 is not related to, and transmit the resultant  
13 content 14 to the service provider 10 (step (5)). In  
14 this manner, the preparation and transmission of the  
15 certificates are completed.

16 Upon the receipt of the certificates from the witnesses  
17 or the certificate generators 12a, the service provider  
18 10 performs a unique non-variable individual or  
19 collective process for the certificates. Subsequently,  
20 each of the resultant certificates, to which the  
21 conditions for the selection of the witness can be  
22 attached, are transmitted to the user 11.

23 Since for the electronic content 14 the process employed  
24 to determine no alteration has occurred is performed not  
25 only by a witness (or a proxy server), but also by the  
26 service provider 10, alteration of the certificate is  
27 extremely difficult, not only by the user 11 and a third  
28 party, but also by the service provider 10 and the

1 witness (or the proxy server) 12a. Therefore, the  
2 validity of the certificate is increased. Further, when  
3 multiple certificates are collected and these  
4 certificates indicate that the content is identical, the  
5 existence (identity) of the content can be proved. As  
6 the number of certificates is increased, so too is the  
7 probative force.

8 Furthermore, when the certificates are continuously  
9 collected and when the contents of the certificates prove  
10 to be identical, the lack of alteration for the pertinent  
11 period can also be proved.

12 The method of this invention will now be described in  
13 detail while referring to the flowchart in Fig. 6, which  
14 shows the general processing performed using the method  
15 of the invention.

16 According to the method of the invention, the rendering  
17 of a service is begun upon the receipt of a service  
18 request from the user 11. First, when the server of the  
19 service provider 10 receives a service request from the  
20 user 11, the server begins a process to identify the user  
21 11 (step 500). The user verification unit 231 in the  
22 certification manager 23 verifies the identity of the  
23 user 11 by referring to the usage history 233. A check  
24 is then performed to determine whether the user 11 is an  
25 authenticated user (step 501), and if it is determined  
26 the user 11 is an authenticated user, program control  
27 shifts to step 502. If the user 11 is not an  
28 authenticated user, an error process is performed and the  
29 processing is thereafter terminated (step 503).

1     Thereafter the service request from the user 11 is  
2     analyzed by the user request analyzation unit 232 in the  
3     certification manager 23 (step 502). A check is  
4     performed to determine whether the request from the user  
5     11 is appropriate (service available) (step 504), and, if  
6     the request is appropriate, program control advances to  
7     step 505. However, if the request is not appropriate, an  
8     error process is performed and the processing is  
9     thereafter terminated (step 506).

10    A member is selected by the registered member selector 25  
11    (step 505), and a check is performed to verify the  
12    selected member is a registered member (step 507). If  
13    the selected member is a registered member, program  
14    control advances to step 508. If the selected member is  
15    not a registered member, an error process is performed  
16    and the processing is thereafter terminated (step 509).

17    Then, the certification process is performed (step 508).  
18    The certification process consists of the dispatch of a  
19    certificate request by the witness process requesting  
20    unit 236 and a process performed by the witness upon the  
21    receipt of the certificate request.

22    A check is performed to determine whether a certificate  
23    has been prepared by the witness (step 510). If a  
24    certificate has been prepared, program control advances  
25    to step 511 for acceptance of the certificate. If a  
26    certificate has not been prepared, program control  
27    returns to step 505 for the selection of a new registered  
28    member.

1 The certificate is subjected to the certificate  
2 acceptance process (step 511). A check is thereafter  
3 performed to determine whether the certificate has been  
4 accepted (step 512). If the certificate has been  
5 accepted, program control advances to step 513 for the  
6 certificate dispatching process. If the certificate has  
7 not been accepted, program control returns to step 505  
8 for the selection of a new registered member.

9 Program control then advances to step 513 for the  
10 certificate dispatching process, and a check is performed  
11 to determine whether the certification period has expired  
12 (step 514). If the certification period has not expired,  
13 while a timer 515 is referred to, program control returns  
14 to step 505 for the selection of a new registered member  
15 at a new certification time, and the certification  
16 process is repeated. When the certification period has  
17 expired, the processing for the service is terminated  
18 (step 516).

19 The individual steps will now be described in detail  
20 while referring to Fig. 7, wherein an example usage  
21 requesting dialogue is shown that is used when the user  
22 11 issues a service request.

23 When the user 11 issues a service request to the service  
24 provider 10, the user 11 enters necessary data in a  
25 dialogue 800 and transmits the data to the service  
26 provider 10. As data to be entered, an address, for  
27 example, of the electronic content 14 to be proved is  
28 entered in an input field 801. The address is written,



1 for example, as a URL, and in this embodiment,  
2 "http://www.ibm.com" is entered. As the profile for the  
3 user 11, a user address is written in an input field 802,  
4 and in this embodiment, an e-mail address,  
5 "test@trl.ibm.com", is entered. As certification  
6 conditions, a period, an accuracy rating, the number of  
7 certificates, the nationality, age and occupation of the  
8 witness, and the proof history are entered in input  
9 fields 803 to 809. These conditions are merely examples,  
10 and not all of them are always required. Furthermore,  
11 other conditions may be added.

12 When the entry of data has been completed, to submit the  
13 data, the user 11 clicks on an "OK" button 810. Or to  
14 cancel the submission of the data, the user 11 clicks on  
15 a "Cancel" button 811.

16 In this example, the input dialogue 800 is shown that is  
17 provided as one part of an application program installed  
18 in the computer system of the user 11. However, a  
19 document for an input screen may be displayed by an  
20 appropriate browser.

21 When the user 11 has clicked on the OK button 810, the  
22 data entered in the input fields are transmitted to the  
23 server of the service provider 10. Upon the receipt of  
24 these data, the server of the service provider 10  
25 initiates a process performed to identify the user 11  
26 (step 500). Fig. 8 is a detailed flowchart showing the  
27 user verification step.

28 First, the address (the return address) of the user 11  
29 that was included in the service request (the input data)

1 is confirmed (step 517). To acknowledge the receipt of  
2 the data and to determine whether a valid return address  
3 was submitted, an e-mail is transmitted to the return  
4 address (step 518). If the e-mail can be delivered,  
5 program control advances to step 519, and if the e-mail  
6 can not be delivered, an error process is performed and  
7 the user verification processing is thereafter terminated  
8 (step 520).

9 Subsequently, the usage history of the user 11 is  
10 examined (step 519). To examine the user history, the  
11 usage history file 233 is employed to determine whether  
12 usage of the user 11 in the past was is satisfactory  
13 (step 521). If the usage in the past was not  
14 satisfactory, e.g., if no payment of a fee is recorded in  
15 the history, data to that effect is stored for the user  
16 in the usage history file 233, and is employed to  
17 determine whether the current usage is appropriate.  
18 Then, if it is found that the usage in the past was  
19 illegal, an error process is performed (step 523). But  
20 if there was no past illegal usage, the current usage is  
21 permitted, and program control advances to step 522. It  
22 should be noted that transmission of a message indicating  
23 that usage was not permitted can be included in the error  
24 process.

25 The method employed for the payment of a commission is  
26 then examined (step 524). An arbitrary payment method  
27 can be employed, such as payment using a credit card, a  
28 transaction service provided through a network using  
29 electronic money or a ticket, or payment from an account  
30 of a user through the money transfer. A check is then

1 performed to determine whether the user is solvent (step  
2 524). When the user is solvent, the user verification  
3 process is terminated, and program control is shifted to  
4 the next step (step 525). When the user is not solvent,  
5 an error process is performed, and the processing is  
6 thereafter terminated (step 526).

7 Fig. 9 is a detailed flowchart showing the user's request  
8 analyzation step (step 502). The timing accuracy  
9 included in the service request (input data) received  
10 from the user 11 is focused on (step 527), and is stored  
11 as a requested timing accuracy (step 528). Similarly,  
12 the proving period, the number of witnesses, the witness  
13 conditions and the proof content address that are entered  
14 are respectively stored as a requested proving period,  
15 the requested number of witnesses, the requested witness  
16 conditions and the requested proof content address (steps  
17 529 to 536). Of course, additional entries can be stored  
18 as requested entries as well. To store the requested  
19 data, a check is performed to determine whether the  
20 request is appropriate. For example, when the timing  
21 accuracy is too high to be attained (e.g., 0.01 second),  
22 when the proving period is too long to be carried out  
23 (e.g., 100 years), or when the number of witnesses  
24 exceeds the number available in the registered member  
25 group, the request is judged inappropriate. An error  
26 process is performed for an inappropriate request, so  
27 that the processing can be terminated. In addition,  
28 whether the type of witness is either a human or a proxy  
29 server can be selected.

30 When the user's request falls within a service available

1 range, the requested proof content address is confirmed  
2 (step 537). During this process, the service provider 10  
3 confirms the presence of the electronic content to be  
4 proved, and attempts to obtain the content to determine  
5 the availability of the content (step 538). If the  
6 acquisition of the content is successful, the presence of  
7 the content is confirmed, and the user's request  
8 analyzation step is terminated (step 539). If the  
9 acquisition of the content fails, the error process is  
10 performed because it is highly probable that the  
11 performance of the succeeding witness process will be  
12 wasted effort. The processing is thereafter terminated  
13 (step 540).

14 Fig. 10 is a detailed flowchart showing the registered  
15 member selection step (step 505). The registered member  
16 database 26 is employed for the selection of a registered  
17 member. The district, the age, the gender, the  
18 occupation and the proof history of the registered member  
19 are stored in the registered member database 26. At this  
20 step, the registered member is selected from the  
21 registered member database 26 in accordance with the  
22 request received from the user 11. That is, based on the  
23 district and age conditions requested by the user 11, the  
24 district condition (step 541), the age condition (step  
25 542), the gender condition (step 543), the occupation  
26 condition (step 544), and the proof history condition  
27 (step 545) are narrowed down. The order in which these  
28 conditions are selected is arbitrary, and while not all  
29 the conditions need at all times be applied, other  
30 conditions may be added.

1 A check is performed to determine whether there are  
2 selected members that match the conditions for the  
3 witnesses (registered members) (whether the required  
4 number of members can be selected) (step 546). If the  
5 required number of registered members can be selected,  
6 program control advances to step 547. If the required  
7 number of registered members can not be selected, an  
8 error process is performed and the processing is  
9 thereafter terminated (step 549). After the registered  
10 members have been selected, a random number is employed  
11 to select a registered member from that group (step 547),  
12 and the selection of the registered member is terminated  
13 (step 548). Since the selection is performed under  
14 predetermined conditions in this manner, the registered  
15 member is selected at random within a requested range  
16 while the request received from the user is satisfied, so  
17 that arbitrariness in the selection of a witness is  
18 eliminated and fairness is ensured. The condition  
19 requiring the narrowing down is not requisite, and  
20 another condition may be added. In addition, the  
21 selection of the registered member need not always be  
22 performed at random; the registered members may be ranked  
23 in accordance with the system conditions established for  
24 the registered members, and may be selected in this  
25 order. Or, in order to uniformly arrange the frequency  
26 whereat registered members are selected, registered  
27 members may be chosen in the ascending order of the  
28 frequency of their prior selection.

29 Fig. 11 is a detailed flowchart showing the proving  
30 process. First, the witness process request is issued by  
31 the service provider 10 to a witness (step 550). This

1 request is transmitted to a witness (or a proxy server  
2 that automatically carries out the witness function) who  
3 was selected during the previous registered member  
4 selection process. The request can be issued by  
5 displaying a dialogue 820 shown in Fig. 12 on the display  
6 screen. The dialogue 820 shown in Fig. 12 is used for  
7 the confirmation of the initiation of the witness  
8 process. A message describing the request for the  
9 preparation of a certificate by the witness, and an OK  
10 button 821 and a Cancel button 822 are displayed in the  
11 dialogue 820. To accept the request, the witness clicks  
12 on the OK button 821, and to refuse the request, the  
13 witness clicks on the Cancel button 822.

14 Upon the receipt of the "OK" or the "Cancel" signal, the  
15 service provider 10 determines whether the witness has  
16 accepted the witness process (step 551). When it is  
17 ascertained that the witness has accepted the witness  
18 process request, program control advances to step 552.  
19 Whereas if it is ascertained the witness has not accepted  
20 the witness process request, an error process is  
21 performed and the processing is thereafter terminated  
22 (step 553).

23 When the system of the witness is a proxy server, a check  
24 can be performed to determine whether the witness process  
25 should be performed by using a predetermined program, and  
26 "OK" or "Cancel" data can be automatically returned to  
27 the server of the service provider.

28 Then, the system of the service provider 10 obtains the  
29 data for clock synchronization (step 552). Clock

1 synchronization is employed to adjust the clocks of the  
2 systems of the service provider and of the witness, and  
3 is performed by referring to an external reference clock.

4 An example external clock service can be  
5 "www.eecis.udel.edu/\_ntp/". Fig. 13A is a block diagram  
6 showing the system of an external clock that is used for  
7 clock synchronization, and Fig. 13B is a flowchart  
8 showing the clock synchronization method. First, the  
9 system of the service provider 10 selects a clock service  
10 (step 558), and attempts to use it to determine whether  
11 the service is available (step 559). If the service is  
12 not available, an attempt is made to use another clock  
13 service (step 561). If that clock service is available,  
14 its address is transmitted to the witness (step 560).  
15 The witness then employs the clock service at the  
16 pertinent address to adjust its own clock (step 562) and  
17 a check is performed to determine whether the service was  
18 available (step 563). If the service was available, a  
19 message indicating a normal end is transmitted to the  
20 service provider (step 564). But if the service was not  
21 available, an error message is returned to the service  
22 provider 10 (step 566), and an attempt is made to use  
23 another clock service.

24 The clock synchronization method has been explained by  
25 using an external clock service; however, an internal  
26 clock may be employed for this purpose. Fig. 14A is a  
27 block diagram showing systems that employ internal clocks  
28 for clock synchronization, and Fig. 14B is a flowchart  
29 showing the clock synchronization method. First, for the  
30 systems of the service provider 10 and the witness 12a,  
31 for which time synchronization units 23a and 30a are

1 included, the time is obtained from the clock 27 of the  
2 service provider 10 (step 567), and the time required for  
3 the transmission of an average packet is calculated (step  
4 568). Then, the time is transmitted by the service  
5 provider 10 to the witness 12a (step 569), whereat the  
6 system receives the time transmitted by the service  
7 provider 10 (step 570). The system of the witness 12a  
8 then corrects the time for the witness 12a, while taking  
9 into account the internal clock 32, the time received  
10 from the service provider 10 and the average packet  
11 transmission time (step 571), and as in this case, the  
12 corrected time is employed for the witness 12a.

13 After clock synchronization has been performed, as is  
14 shown in Fig. 11, the proof condition, which includes the  
15 address of the electronic content but can also include  
16 the form for the preparation of a certificate, e.g.,  
17 information concerning whether hash code should be  
18 generated using a hash function, is transmitted by the  
19 service provider 10 to the witness 12a (step 554).

20 Thereafter, the witness 12a prepares a certificate (step  
21 555). Fig. 15 is a detailed flowchart showing the  
22 certificate generation step.

23 First, the witness 12a accesses the content address that  
24 was transmitted at the proof condition transmission step  
25 (step 554), and attempts to obtain the electronic content  
26 14 (step 572). For this, a check is performed to  
27 determine whether the electronic content 14 could be  
28 obtained (step 573). If the acquisition of the  
29 electronic content 14 is successful, program control



1 advances to step 576, but if the electronic content 14  
2 can not be obtained, another attempt is made to acquire  
3 the electronic content 14 (step 574), and program control  
4 returns to step 572. When the number of retries reaches  
5 a predetermined count, it is assumed that acquisition of  
6 the electronic content 14 has failed and an error process  
7 is performed and the processing is thereafter terminated  
8 (step 575).

9 After the electronic content 14 is obtained, the  
10 acquisition of the time is attempted (step 576) and a  
11 check is performed to determine whether the acquisition  
12 of the time was successful (step 577). When the time has  
13 been acquired, program control advances to step 580, but  
14 if the time can not be obtained, another attempt is made  
15 to acquire the time (step 578) and program control  
16 returns to step 576. When the number of retries reaches  
17 a predetermined count, it is assumed that the acquisition  
18 of the time has failed, and an error process is performed  
19 and the processing is thereafter terminated (step 579).

20 The obtained electronic content 14 and time are assembled  
21 with the content address to form the data 331 (step 580),  
22 and an electronic signature is provided for the data 331  
23 (step 581) and the certificate preparation step is  
24 thereafter terminated.

25 Fig. 16 is a diagram showing a display screen for a  
26 certificate preparation dialogue box at the preceding  
27 step of provision of an electronic signature. In a  
28 dialogue box 830, the address of the electronic content  
29 14 is displayed in a field 831 and the electronic content

1 14 is displayed in a field 832. The results obtained by  
2 accessing the pertinent address, i.e., a message  
3 inquiring as to whether the proof can be provided for the  
4 content, and an OK button 834 and a Cancel button 835 are  
5 displayed that are used to request confirmation that the  
6 certificate has been issued. When the witness 12a clicks  
7 on the OK button 834, the certificate with an electronic  
8 signature is issued.

9 Fig. 17 is a detailed flowchart showing the electronic  
10 signature step. At step 580, data consisting of the  
11 content address, and the electronic content and the time  
12 are generated, and at step 582 hash code for this data is  
13 generated. Since the data is converted into hash code,  
14 the certificates can be distinguished between by  
15 examining the hash code, so that the determination can be  
16 easily performed. It should be noted that, as in the  
17 previous explanation of the system, the conversion of  
18 data into hash code need not always be performed. When  
19 the data satisfies a unique conversion condition, a  
20 function other than the hash function may be employed.  
21 However, when the data is not converted into hash code,  
22 or when another function is employed for code conversion,  
23 at the next step the data consisting of the content  
24 address, the electronic content and the time, or the code  
25 obtained by conversion, should be encrypted.

26 The hash code is encrypted by using the secret key (step  
27 583). Since the secret key that only the witness 12a  
28 knows is employed to encrypt the hash code, alteration of  
29 the certificate is substantially impossible for anybody  
30 but the witness 12a. As will be described later, the

1 certificate is further encrypted by the service provider  
2 by using a secret key. Since the certificate is  
3 encrypted twice, alteration of the certificate provided  
4 for the user 11 is impossible for both the witness 12a  
5 and the service provider 10. As a result, there is  
6 increased reliability that the certificate has not been  
7 altered.

8 The electronic content, the content address and the time  
9 are added to the hash code that is encrypted using the  
10 secret key (step 584), and the electronic signature  
11 process is terminated. And through the witness process,  
12 the certificate is generated. The public key of the  
13 public key registration service provider 10 can be  
14 attached to the certificate, so that the communication of  
15 the encrypted certificate can be safely performed.

16 The thus generated certificate is returned to the  
17 certification manager 23 in the service provide 10, as is  
18 shown in Fig. 11 (step 556). The proof process is  
19 thereafter terminated.

20 Fig. 18 is a detailed flowchart showing the certificate  
21 acceptance step. When the server of the service provider  
22 10 receives a certificate from the witness 12a, the time  
23 for requesting the proof process, the time attached to  
24 the certificate and the current time are compared with  
25 each other (step 585), and a check is performed to  
26 determine whether the time difference satisfies the  
27 request from the user 11 (step 586). If the request is  
28 satisfied, program control advances to step 587. If the  
29 request is not satisfied, an error process is performed

1 and the processing is thereafter terminated (step 588).

2 The electronic content attached to the certificate is  
3 compared with the electronic content that was previously  
4 obtained by the service provider 10 (step 587), and  
5 determines whether the electronic contents are matched  
6 (step 589). When the two electronic contents are  
7 matched, program control advances to step 590, while when  
8 the electronic contents are not matched, an error process  
9 is performed and the processing is thereafter terminated  
10 (step 591). It should be noted that hash code can be  
11 employed for determining whether the electronic content  
12 are identical. When multiple certificates are present,  
13 they can be compared with each other instead of the  
14 content previously obtained by the service provider 10.

15 The witness signature of the witness on the certificate  
16 is examined (step 590) to determine whether the witness  
17 signature is correct (step 592). If the signature is  
18 correct the electronic signature of the service provider  
19 10 is additionally attached (step 593), and the  
20 certificate acceptance step is terminated. If the  
21 electronic signature on the certificate is not correct,  
22 an error process is performed and the certificate  
23 acceptance step is terminated (step 594).

24 Since not only the signature of the witness, but also the  
25 signature of the service provider is added to the  
26 certificate, alteration of the certificate is impossible  
27 for both the third party and the user 11, and also for  
28 the service provider and the witness. Thus, high  
29 reliability can be maintained for the certificate, and

1 the probative force of the certificate can be increased.

2 A service provided by, for example,  
3 "www.moj.go.jp/PUBLIC/MINJI02/pub\_minji02\_04.htm" is  
4 employed as the electronic signature; however, any  
5 electronic signature may be employed so long as it is  
6 ensured with a signature that the data has not been  
7 altered.

8 Fig. 19 is a diagram showing a display screen for the  
9 final stage of the preparation of a certificate by the  
10 service provider 10. Bibliographical data, such as the  
11 person who issued the content and the proof date, are  
12 entered in a file 841 for a frame 840, and the electronic  
13 content is displayed in a field 842. Finally, in a field  
14 843 hash codes provided by the witness 12a and the  
15 service provider 10 are displayed.

16 As is shown in Fig. 20, multiple electronic contents can  
17 be displayed in one certificate. In Fig. 20,  
18 bibliographical matters, such as the person who issued  
19 the electronic content and the proof date, are displayed  
20 in a field 851 of a frame 850, and multiple electronic  
21 contents are displayed in fields 852 to 855. The hash  
22 codes obtained by the witness 12a and the service  
23 provider 10 are displayed in a field 856.

24 Fig. 21 is a detailed flowchart showing the certificate  
25 dispatching step. Before transmitting the certificate to  
26 the user 11, the service provider 10 determines whether a  
27 notary service is to be employed (step 595). If a notary  
28 service is employed, the notary service is received at

1 step 596, and program control advances to step 597. If  
2 the notary service is not necessary, program control  
3 skips step 596 and jumps to step 597. A check is then  
4 performed to determine whether a certificate accumulation  
5 service is to be employed (step 597). If this service is  
6 to be employed, the certificate accumulation service is  
7 received at step 598, and program control advances to  
8 step 599. If the certificate accumulation service is not  
9 necessary, program control skips step 598 and jumps to  
10 step 599. Finally, the certificate is transmitted to the  
11 user 11 (step 599).

12 The proving method of this invention is completed in this  
13 manner. According to this method, the evidence for the  
14 presence of the electronic content can be collected by  
15 using the above described system. Therefore, not only  
16 the presence of the electronic content, but also the  
17 continuous presence of the same electronic content, i.e.,  
18 that the electronic content has not been altered, can be  
19 proved. Further, since the witness or the proxy sever is  
20 a third party unrelated to the user, the fact is that,  
21 even strictly speaking, it can be proven that the  
22 electronic content has been opened for perusal. That is,  
23 strictly speaking, the electronic content has not been  
24 opened for perusal, even though the conventional proving  
25 institution proves the content has been opened for that  
26 institution. However, the witness or the proxy server  
27 for this invention is an unspecified third party and can  
28 be regarded as the public, and since the electronic  
29 content has been opened for perusal by the witness, it  
30 can therefore be proven that, even strictly speaking, the  
31 electronic content has been opened for perusal (made

1 available to the public).

2 If the proving period is extended for a long time, the  
3 identity of the electronic content can be proven for a  
4 period before and after a specific date by using the  
5 above certificate or multiple certificates, and it can  
6 also be proven that the electronic content was altered at  
7 a specific date. Specifically, the certificates are  
8 collected continuously, and when an alteration of the  
9 electronic content or the hash code attached to the  
10 certificate was found at a specific date, it can be  
11 proven that the electronic content was changed on the  
12 specific date. In other words, non-alteration before the  
13 specific date, the alteration date, and non-alteration  
14 following the specific date can be proved. Further, when  
15 alterations were made a plurality of times, the  
16 alteration dates and the period during which the  
17 identical content was maintained can be proven.

18 The registration of a witness can be performed as  
19 follows. Fig. 22A is a block diagram showing a witness  
20 registration system, and Fig. 22B is a flowchart showing  
21 a witness registration method. The service provider 10  
22 and the certificate generator 12a are employed for this  
23 processing. The server of the service provider 10  
24 comprising a registered member database 40, a witness  
25 registration manager 41 and a communication unit 42, and  
26 the certificate generator 12a including a communication  
27 unit 43 and a witness registration unit 44. First, via  
28 the communication units 43 and 42, the certificate  
29 generator 12a issues a witness registration request to  
30 the service provider 10, and the service provider 10

1 accepts this request (step 600). Thereafter, the witness  
2 registration manager 41 of the service provider 10  
3 examines this witness (step 601) to determine whether the  
4 witness satisfies the registered member condition (step  
5 602). If the witness satisfies the condition, the  
6 witness is registered in the registered member database  
7 40, and the processing is thereafter terminated (step  
8 603). If the witness does not satisfy the condition, an  
9 error process is performed and the processing is  
10 thereafter terminated (step 604).

11 (Second Embodiment)

12 Fig. 23 is a conceptual diagram showing an example  
13 proving system according to a second embodiment of the  
14 present invention. In this embodiment, a service  
15 provider 10, a user 11, a registered member group 12, a  
16 witness or certificate generator 12a, a content  
17 transmitter 13 and an electronic content 14 are the same  
18 as those in the first embodiment, and in addition, and  
19 electronic notary service provider 900 is employed. The  
20 electronic notary service provider 900 furnishes a notary  
21 service provided, for example, by "www.surety.com", and  
22 ensures the probative force of the certificate by using  
23 the credibility of a notary public instead of the  
24 electronic signature in the first embodiment. In the  
25 explanation that follows, a description of the components  
26 and processes of this embodiment that correspond to like  
27 elements of the first embodiment will not be given.

28 Fig. 24 is a block diagram showing an example service  
29 provider and an example certificate generator according  
30 to the system for the second embodiment. Fig. 25 is a



1 block diagram showing an example certificate generation  
2 manager and an example certification generation  
3 processor. The service provider 10 (a certificate  
4 request receiver 21, a certificate transmitter 22, a  
5 certification manger 23, a communication unit 24, a  
6 registered member selector 25, a registered member  
7 database 26, a clock 27 and an electronic content  
8 acquisition unit 28) is the same as that in the first  
9 embodiment. And the certificate generator 12a includes a  
10 communication unit 29, a certificate generation manager  
11 30, an electronic content acquisition unit 31, a clock 32  
12 and a certification generation processor 33, as in the  
13 first embodiment.

14 In the second embodiment, the notary service provider 900  
15 is included as a component for the proof service method  
16 and system. As is explained in the first embodiment, the  
17 certification manager 23 and the certification generation  
18 processor 33 add an electronic signature for the service  
19 provider 10 and the certificate generator 12a. In this  
20 embodiment, authentication by the notary service provider  
21 900 is employed instead of an electronic signature.  
22 Thus, the system of this invention does not includes the  
23 electronic signature generator 34 used in the first  
24 embodiment.

25 As is shown in Fig. 25, the certificate generation  
26 manager 30 prepares a witness profile 901, in addition to  
27 the content address 212, the electronic content 302 and  
28 the time 303 explained in the first embodiment.

29 The certification generation processor 33 generates data

1 902 from the content address 212, the electronic content  
2 302, the time 303 and the witness profile 901, and to  
3 request authentication, transmits the data 902 to the  
4 electronic notary service provider 900. Thereafter, the  
5 authenticated data are transmitted as a certificate 903  
6 by the electronic notary service provider 900 to the  
7 certification generation processor 33, and the  
8 certificate 903 is then issued to the service provider  
9 10.

10 According to the embodiment, even without the electronic  
11 signature of the witness or the service provider, the  
12 non-alteration of the certificate is ensured by the  
13 authentication furnished by the notary service provider  
14 900. The alteration of the certificate 903 by the user  
15 and the third party is impossible, and the probative  
16 force of the certificate 903 can be effectively obtained.

17 The present invention has been explained by referring to  
18 the embodiments; however, the present invention is not  
19 limited to these embodiment, and can be variously  
20 modified without departing from the scope of the  
21 invention.

22 For example, as is shown in Fig. 26, the user 11 and the  
23 content transmitter 13 (electronic content 14) may be  
24 included in the same computer system.

25 Further, as is shown in Fig. 27, the present invention  
26 may be employed to prove the electronic content 14 that  
27 is owned by the service provider 10. In this case, since  
28 the user 11 and the service provider 10 are constituted  
29 using the same computer system, the use by the means in

1 the first embodiment of the electronic signature of the  
2 service provider to prevent the alteration of the  
3 certificate is not the preferable solution. In order to  
4 prevent the alteration of the certificate, i.e., to  
5 increase the probative force of the certificate, it is  
6 preferable that authentication by the notary service  
7 provider be obtained.

8 The non-alteration of the certificate is ensured by using  
9 the double electronic signatures of the service provider  
10 and the witness in the first embodiment, and by using the  
11 authentication furnished by the notary institution in the  
12 second embodiment. However, the double electronic  
13 signatures of a witness or a service provider and of a  
14 third party other than the service provider, the user and  
15 the witness may be employed. Further, the notary service  
16 may be accepted in addition to the double electronic  
17 signatures.

18 In conclusion, the following matters are disclosed for  
19 the configuration of the present invention.

20 (1) An electronic content proving method using a computer  
21 system or a computer network comprising the steps of: (a)  
22 a proof service provider transmitting a certificate  
23 generation request to a witness or a certificate  
24 generator; (b) the witness or the certificate generator  
25 obtaining electronic content upon the receipt of the  
26 certificate generation request from the service provider;  
27 and (c) generating a certificate.

28 (2) The electronic content proving method according to  
29 (1), wherein the certificate includes the electronic  
30 content, or data that uniquely represent the electronic

1 content.

2 (3) The electronic content proving method according to  
3 (1) or (2), further comprising the step of (d)  
4 accumulating the certificate in the service provider or  
5 transmitting the certificate to a user.

6 (4) The electronic content proving method according to  
7 one of (1) to (3), wherein the certificate includes  
8 address information for the electronic content and time  
9 information for the proof.

10 (5) The electronic content proving method according to  
11 one of (1) to (4), wherein the step of generating the  
12 certificate includes a step of providing a signature for  
13 the certificate.

14 (6) The electronic content proving method according to  
15 (5), wherein the signature step includes a first  
16 configuration process consisting of a first signature  
17 step by the witness or the certificate generator and a  
18 second signature step by the service provider, or a  
19 second configuration process consisting of a signature  
20 step by a notary service provider.

21 (7) The electronic content proving method according to  
22 (5) or (6), wherein the signature is encrypted using a  
23 public key encryption method to prevent alteration by a  
24 person other than a signer.

25 (8) The electronic content proving method according to  
26 one of (5) to (7), wherein the signature is provided by  
27 using a secret key belonging to the witness, the  
28 certificate generator or the service provider.

29 (9) The electronic content proving method according to  
30 one of (2) to (8), wherein the data that uniquely  
31 represents the electronic content is a hash code.

32 (10) The electronic content proving method according to

1 one of (1) to (9), wherein, before transmission of the  
2 certificate, a public key belonging to a public key  
3 authentication service provider is added to the  
4 certificate.

5 (11) The electronic content proving method according to  
6 one of (1) to (10), wherein a service request received  
7 from the user includes the address information for the  
8 electronic content, request information concerning an  
9 attribute of the witness, and request information  
10 concerning the proof.

11 (12) The electronic content proving method according to  
12 one of (1) to (11), wherein in accordance with a request  
13 from the user, the certificate generation request is  
14 transmitted to the witness or to the certificate  
15 generator on one or multiple dates, or is transmitted  
16 continuously during one or multiple specific periods.

17 (13) The electronic content proving method according to  
18 one of (1) to (12), wherein the witness or the  
19 certificate generator includes either a first  
20 configuration that is selected at random, a second  
21 configuration that is selected from a set of witnesses or  
22 certificate generators that satisfy a request received  
23 from the user, or a third configuration that is selected  
24 at random from a set of witnesses or certificate  
25 generators that satisfy a request received from the user.

26 (14) The electronic content proving method according to  
27 one of (1) to (13), wherein synchronization of time is  
28 effected between the service provider and the witness or  
29 the certificate generator.

30 (15) The electronic content proving method according to  
31 (14), wherein the time synchronization is effected by  
32 employing a method that uses either an external clock

1 service or a method for employing an average packet  
2 transmission time to correct the internal clocks of the  
3 service provider and the witness or the certificate  
4 generator.

5 (16) A proving system for a service provider that proves  
6 oneness for perusal and non-alteration of an electronic  
7 content using a computer system or a computer network  
8 comprising: means for transmitting a certificate  
9 generation request to a witness or a certificate  
10 generator; means for obtaining electronic content upon  
11 the receipt of the certificate generation request from  
12 the service provider; and means for generating a  
13 certificate.

14 (17) The proving system according to (16), wherein the  
15 certificate includes the electronic content, or data that  
16 uniquely represent the electronic content.

17 (18) The proving system according to (16) or (17),  
18 further comprising: means for accumulating the  
19 certificate in a computer system of the service provider  
20 or means for transmitting the certificate to a user.

21 (19) The proving system according to one of (16) to (18),  
22 wherein the certificate includes address information for  
23 the electronic content and time information for the  
24 proof.

25 (20) The proving system according to one of (16) to (19),  
26 wherein the means for generating the certificate includes  
27 means for providing a signature for the certificate.

28 (21) The proving system according to (20), wherein the  
29 signature means includes a first configuration consisting  
30 of first signature means by the witness or the  
31 certificate generator and second signature means by the  
32 service provider, or a second configuration consisting of

1 signature means by a notary service provider.

2 (22) The proving system according to (20) or (21),  
3 wherein encryption means using a public key encryption  
4 method is employed for the signature means to prevent  
5 alteration by a person other than a signer.

6 (23) The proving system according to one of (16) to (22),  
7 wherein the signature is provided by using a secret key  
8 belonging to the witness, the certificate generator or  
9 the service provider.

10 (24) A proving system for a service provider that proves  
11 openness for perusal or non-alteration of an electronic  
12 content using a computer system or a computer network,  
13 comprising: means for accepting and for analyzing a  
14 service request received from a user; means for selecting  
15 a witness or a certificate generator from a registered  
16 member group in which witnesses or certificate generators  
17 are registered; means for transmitting a certificate  
18 generation request to the witness or the certificate  
19 generator that is selected; means for accepting a  
20 certificate from the witness or from the certificate  
21 generator; and means for transmitting the certificate to  
22 the user.

23 (25) The proving system according to (24), wherein the  
24 means for accepting the certificate includes means for  
25 providing an electronic signature for the certificate.

26 (26) The proving system according to (25), wherein the  
27 electronic signature is means for encrypting the  
28 certificate using a secret key belonging to the service  
29 provider.

30 (27) The proving system according to one of (24) to (26),  
31 wherein the service request includes a condition  
32 concerning the witness; and wherein a first configuration

1 that includes means for selecting a group of witnesses  
2 satisfying the condition concerning the witness, or a  
3 second configuration including means for selecting the  
4 witness or the certificate generator at random is  
5 provided as the means for selecting the witness or the  
6 certificate generator.

7 (28) The proving system according to one of (24) to (27),  
8 wherein the service request includes a date or a period  
9 for the proof, and wherein the means for transmitting the  
10 certificate generation request includes means for  
11 continuously transmitting the certificate generation  
12 request for the date or during the period.

13 (29) A system for a witness or a certificate generator  
14 that proves openness for perusal or non-alteration of an  
15 electronic content using a computer system or a computer  
16 network, comprising: means for accepting a certificate  
17 generation request from a user; means for accessing an  
18 address of an electronic content included in the  
19 certificate generation request, and obtaining the  
20 electronic content; means for generating a certificate  
21 including the electronic content, or code that uniquely  
22 represents the electronic content; and means for  
23 transmitting the certificate to the service provider.

24 (30) The system according to (29), wherein the means for  
25 generating the certificate includes means for providing  
26 an electronic signature for the certificate.

27 (31) The system according to (30), wherein the electronic  
28 signature is means for encrypting the certificate using a  
29 secret key belonging to the witness or the certificate  
30 generator.

31 (32) The system according to one of (29) to (31), wherein  
32 the code that uniquely represents the electronic content



1 is a hash code.

2 (33) The system according to one of (29) to (32), wherein  
3 the means for generating the certificate includes means  
4 for adding time information that is synchronized with a  
5 clock of the service provider.

6 (34) A storage medium for storing a program code that  
7 proves openness for perusal and non-alteration of an  
8 electronic content using a computer system or a computer  
9 network, the program code comprising: a program code for,  
10 in accordance with a service request from a user or a  
11 self service request, transmitting a certificate  
12 generation request to a witness or a certificate  
13 generator; a program code for obtaining electronic  
14 content upon the receipt of the certificate generation  
15 request from the service provider; a program code for  
16 generating a certificate that includes the electronic  
17 content, or data that uniquely represent the electronic  
18 content; and either a program code for accumulating the  
19 certificate in a computer system of the service provider  
20 or a program code for transmitting the certificate to a  
21 user.

22 (35) A storage medium for storing a program code that  
23 proves openness for perusal and non-alteration of an  
24 electronic content using a computer system or a computer  
25 network, the program code comprising: a program code for  
26 accepting and for analyzing a service request received  
27 from a user; a program code for selecting a witness or a  
28 certificate generator from a registered member group in  
29 which witnesses or certificate generators are registered;  
30 a program code for transmitting a certificate generation  
31 request to the witness or the certificate generator that  
32 is selected; a program code for accepting a certificate

1 from the witness or from the certificate generator; and a  
2 program code for transmitting the certificate to the  
3 user.

4 (36) A storage medium for storing a program code that  
5 proves openness for perusal and non-alteration of an  
6 electronic content using a computer system or a computer  
7 network, the program code comprising: a program code for  
8 accepting a certificate generation request from a service  
9 provider; a program code for accessing an address of an  
10 electronic content included in the certificate generation  
11 request, and obtaining the electronic content; a program  
12 code for generating a certificate including the  
13 electronic content, or code that uniquely represents the  
14 electronic content; and a program code for transmitting  
15 the certificate to the service provider.

16 The following effects are obtained by the present  
17 invention: Means can be provided for testifying to the  
18 openness for perusal of the electronic content that is  
19 available on a network. Further, means is provided for  
20 testifying that electronic content available on a network  
21 has not been altered. Furthermore, the probative force  
22 needed to demonstrate the openness for perusal or the  
23 lack of alteration of electronic content can be  
24 increased.

25 The present invention can be realized in hardware,  
26 software, or a combination of hardware and software. The  
27 present invention can be realized in a centralized fashion  
28 in one computer system, or in a distributed fashion where  
29 different elements are spread across several interconnected  
30 computer systems. Any kind of computer system - or other

1 apparatus adapted for carrying out the methods described  
2 herein - is suitable. A typical combination of hardware and  
3 software could be a general purpose computer system with a  
4 computer program that, when being loaded and executed,  
5 controls the computer system such that it carries out the  
6 methods described herein. The present invention can also be  
7 embedded in a computer program product, which comprises all  
8 the features enabling the implementation of the methods  
9 described herein, and which - when loaded in a computer  
10 system - is able to carry out these methods.

11 Computer program means or computer program in the present  
12 context mean any expression, in any language, code or  
13 notation, of a set of instructions intended to cause a  
14 system having an information processing capability to  
15 perform a particular function either directly or after  
16 conversion to another language, code or notation and/or  
17 reproduction in a different material form.

18 It is noted that the foregoing has outlined some of the  
19 more pertinent objects and embodiments of the present  
20 invention. This invention may be used for many  
21 applications. Thus, although the description is made for  
22 particular arrangements and methods, the intent and  
23 concept of the invention is suitable and applicable to  
24 other arrangements and applications. It will be clear to  
25 those skilled in the art that other modifications to the  
26 disclosed embodiments can be effected without departing  
27 from the spirit and scope of the invention. The described  
28 embodiments ought to be construed to be merely illustrative  
29 of some of the more prominent features and applications of  
30 the invention. Other beneficial results can be realized by

1     applying the disclosed invention in a different manner or  
2     modifying the invention in ways known to those familiar  
3     with the art.